STEPHANIE M. HINDS (CABN 154284)
Acting United States Attorney

HALLIE HOFFMAN (CABN 210020)
Chief, Criminal Division

DAVID COUNTRYMAN (CABN 226995)
CHRIS KALTSAS (NYBN 5460902)
CLAUDIA A. QUIROZ (CABN 254419)
WILLIAM FRENTZEN (LABN 24421)
Assistant United States Attorneys

450 Golden Gate Avenue, Box 36055
San Francisco, California 94102-3495
Telephone: (415) 436-436-7428
FAX: (415) 436-7234
claudia.quiroz@usdoj.gov

Attorneys for United States of America

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. Approximately 69,370 Bitcoin (BTC), Bitcoin Gold (BTG), Bitcoin SV (BSV), and Bitcoin Cash (BCH) seized from 1HQ3Go3ggs8pFnXuHVHRytPCq5fGG8Hbhx Defendant. ILIJA MATUSKO, Claimant.	CASE NO. CV 20-7811 RS **DECLARATION OF JEREMIAH HAYNIE IN SUPPORT OF UNITED STATES' MOTION TO STRIKE THE VERIFIED CLAIM OF CLAIMANT ILIJA MATUSKO** Hearing Date: September 9, 2021 Time: 1:30 p.m. Court: Hon. Richard Seeborg

I, JEREMIAH HANYIE, state as follows:

1. I am a Special Agent with the Criminal Investigation Division of the Internal Revenue Service ("IRS-CI"). I am a case agent assigned to this case. I respectfully submit this declaration to provide certain relevant information in support of the United States' Motion to Strike the Verified Claim of Ilija Matusko. I personally conducted the blockchain analysis of the bitcoin at issue in this case and was involved in the investigation from its inception to the present day.

2. From its inception in 2011 until October 2013, when it was seized by law enforcement, Silk Road was the most sophisticated and extensive criminal marketplace on the Internet, serving as a sprawling black-market bazaar where unlawful goods and services, including illegal drugs of virtually all varieties, were bought and sold regularly by the site's users. During its two-and-a-half years in operation, Silk Road was used by thousands of drug dealers and other unlawful vendors to distribute hundreds of kilograms of illegal drugs and other unlawful goods and services to well over 100,000 buyers, and to launder hundreds of millions of dollars derived from these unlawful transactions.

3. For example, contemporaneous with its seizure, there were nearly 13,000 listings for controlled substances on the website, listed under the categories "Cannabis," "Dissociatives," "Ecstasy," "Intoxicants," "Opioids," "Precursors," "Prescription," "Psychedelics," and "Stimulants," among others. Clicking on the link for a particular listing brings up a picture and description of the drugs being offered for sale, such as "HIGH QUALITY #4 HEROIN ALL ROCK" or "5gr UNCUT Crystal Cocaine!!". Nearly 95% of all sales on Silk Road were for illegal drugs.

4. During its operation, law enforcement agents made over 100 individual undercover purchases of controlled substances from Silk Road vendors. The substances purchased in these undercover transactions have been various Schedule I and II drugs, including ecstasy, cocaine, heroin, LSD, and others. Samples of these purchases were laboratory-tested and have typically shown high purity levels of the items that were advertised by Silk Road. Based on the postal markings of the packages in which the drugs arrived, these purchases appear to have been filled by vendors located in over ten different countries, including the United States. Law enforcement agents also made undercover purchases of hacking services on Silk Road, including purchases of malicious software such as password stealers and remote access tools.

5. Contemporaneous with the seizure of Silk Road, there were 159 listings on the site under the category "Services." Most concerned computer services: for example, one listing was by a vendor to hack into Facebook, Twitter, and other social networking accounts of the customer's choosing, offering that "You can Read, Write, Upload, Delete, View All Personal Info"; another offered tutorials teaching "22 different methods" for hacking ATM machines. Other listings offered services that were likewise criminal in nature. For example, one listing was for "HUGE Blackmarket Contact List," which described lists of "connects" for "Services" such as "Anonymous Bank Accounts," "Counterfeit Bills (CAD/GBP/EUR/USD)," "Firearms + Ammunition," "Stolen Info (CC [credit card], Paypal)," and "Hitmen (10+ countries)."

6. Silk Road was owned and operated by its creator Ross William Ulbricht, a/k/a "Dread Pirate Roberts," a/k/a "DPR," a/k/a "Silk Road" (hereinafter "Ulbricht"). Ulbricht controlled and oversaw all aspects of Silk Road. He maintained the computer infrastructure and programming code underlying the Silk Road website; he determined vendor and customer policies, including deciding what could be sold on the site; he managed a small staff of online administrators who assisted with the day-to-day operations of the site; and he alone controlled the massive profits generated from the operation of the business. The contents of the Silk road web server included Ulbricht's own user account page, which reflected, among other things, his history of Bitcoin transactions on the site. Ulbricht's transaction history reflects that he received a continuous flow of Bitcoins into his Silk Road account. For example, on July 21, 2013 alone, Ulbricht received approximately 3,237 separate transfers of Bitcoins into his account. Virtually all of those transactions were labeled "commission" in the "notes" appearing next to them, indicating that the money represented commissions from Silk Road sales. Ulbricht's account page further displayed the total amount of Bitcoins deposited in his Silk Road account, which, as of July 23, 2013, equaled more than $3.4 million. Thus, Ulbricht received a steady stream of commissions from Silk Road in the form of Bitcoins. The government's investigation in that case did not uncover any legitimate sources of income for Ulbricht at the time of his arrest.

7. The only form of payment accepted on Silk Road was bitcoin. Upon registering an account with Silk Road, users were assigned a Bitcoin address. Bitcoin sent to the user's Bitcoin address was credited to the user's account. According to the Silk Road wiki web page, Silk Road used a

"tumbler" to send "all payments through a complex, semi-random series of dummy transactions, . . . making it nearly impossible to link your payment with any coins leaving the site." In other words, if a buyer makes a payment on Silk Road, the tumbler obscures any link between the buyer's Bitcoin address and the vendor's Bitcoin address where the bitcoin end up—making it fruitless to use the Blockchain to follow the money trail involved in the transaction, even if the buyer's and vendor's Bitcoin addresses are both known. The only function served by Silk Road's implementation of such "tumblers" is to assist with the laundering of criminal proceeds. All told, Silk Road generated sales revenue totaling over 9.5 million bitcoin, and collected commissions from these sales totaling over 600,000 bitcoin. The figures were, at the time of Ulbricht's initial charges by complaint, equivalent to approximately $1.2 billion in sales and approximately $80 million in commissions.[1]

8. On October 1, 2013, Ulbricht was arrested in San Francisco, California and charged in the Southern District of New York via a criminal Complaint with narcotics trafficking conspiracy, computer hacking conspiracy, and money laundering conspiracy.[2] Having located a server containing the corresponding authentication key for the Silk Road website on the Tor network, law enforcement simultaneously took down the website and seized its servers, including all bitcoins contained in wallets residing within them. Below is an image of the takedown notice placed on the Silk Road website:

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

[1] Under today's valuation, with a price per Bitcoin of $31,774.20 USD, that would be equivalent to $302 billion in sales and approximately $19 billion in commissions.

[2] Ulbricht had moved to San Francisco, within the Northern District of California, prior to his arrest and was operating Silk Road from the Northern District of California. After his arrest he was processed through the United States District Court for the Northern District of California before being removed to the Southern District of New York for prosecution. At the time of his arrest, Ulbricht was using a laptop, which was seized in connection with his arrest. A subsequent search of his residence revealed several pieces of computer hardware belonging to him. Federal law enforcement agents recovered from the computer hardware a Bitcoin wallet containing approximately 144,336 Bitcoins.

9. On approximately May 6, 2012, Individual X stole 70,411.46 BTC from addresses controlled by Silk Road and transferred it to two Bitcoin addresses—1BADznNF3W1gi47R65MQs754KB7zTaGuYZ (hereafter "1BAD") and 1BBqjKsYuLEUE9Y5WzdbzCtYzCiQgHqtPN (hereafter "1BBq"). Individual X used a vulnerability that allowed him to withdraw funds from Silk Road without authorization. The transfers to 1BAD and 1BBq came from the general pool of Silk Road bitcoin and not from any particular user accounts. Meaning after these transfers were made, no user balances were impacted including the balance of hanson5.

10. This is different from another notable theft of bitcoin from Silk Road, namely that by former U.S. Secret Service Special Agent Shaun Bridges. Bridges was involved in the investigation and arrest of a Silk Road moderator. The moderator provided the investigation team, including Bridges, with his Silk Road administrative login credentials. Bridges used these credentials to reset specific vendor passwords which allowed him to take over the accounts of multiple Silk Road vendors. Bridges used his access to the vendor accounts to withdraw bitcoin contained within the accounts to Bitcoin addresses he controlled. The difference here is that Bridges stole bitcoin from specific Silk Road vendor

accounts and the balances of those accounts were reduced accordingly within the Silk Road database. Individual X, on the other hand, stole bitcoin from a pool of Silk Road bitcoin. Therefore, no particular vendor or user accounts were impacted.

11. Further, after Ulbricht realized that funds had been stolen from particular vendors during the Bridges theft, Ulbricht restored the vendors' balance back to what it was pre-theft. Contrarily, after Individual X stole from Silk Road, Ulbricht did not need to restore account balances because the theft was not from any particular Silk Road account. In addition, Ulbricht did not disclose the theft of bitcoin and the theft did not have an impact on the users' ability to withdraw.

12. The theft of bitcoin by Individual X had no impact on the hanson5 Silk Road account balance. A copy of the Silk Road server when it was seized in October 2013 showed that the hanson5 account received 47.52 bitcoin in December 2011. The hanson5 Silk Road account had the same balance when the server was seized in October 2013. Notedly, the account was unaffected when Individual X stole bitcoin from Silk Road in May 2012. At any time from December 2011 to October 2013, the owner of the hanson5 account could have withdrawn bitcoin from the account.

BITCOIN OVERVIEW

13. Through my training and experience, and through reference to open-source information available via the Internet, I know the following:

14. Bitcoin is a type of virtual currency.[3] Virtual currency (also known as cryptocurrency or digital currency) is a digital representation of value that can function as a medium of exchange, a unit of account, and/or a store of value.[4] Virtual currency is not issued by any government or bank. It is generated and controlled through computer software operating on a decentralized, peer-to-peer network. Virtual currency is not illegal in the United States and may be used for legitimate financial transactions. However, virtual currency is frequently used in conjunction with illegal or restricted activities,

[3] Bitcoin is both a cryptocurrency and a protocol; because of this, capitalization differs. Accepted practice is to use "Bitcoin" (singular with an uppercase letter B) to label the protocol, software, and community, and "bitcoin" (with a lowercase letter b) to label units of the currency. That practice is adopted here.

[4] For the purposes of this affidavit, "digital currency," "cryptocurrency," and "virtual currency" address the same concept.

including, for example, purchasing illegal narcotics on darknet markets.

15. To send and receive bitcoin, the parties involved in a transaction use Bitcoin "addresses." A Bitcoin address is somewhat analogous to a bank account number and is represented as a 26-to-35-character-long case-sensitive string of letters and numbers. Each Bitcoin address is controlled through the use of a unique, private key. This key is the equivalent of a password or PIN and is necessary to access the funds associated with a Bitcoin address. Only the holder of a Bitcoin address' private key can authorize transfers of bitcoin from that address to other Bitcoin addresses. Users can operate multiple Bitcoin addresses at any given time and can use a unique Bitcoin address for each transaction.

16. When a sender initiates a Bitcoin transaction, the sender transmits a transaction announcement across the peer-to-peer Bitcoin network. To complete a transaction, a sender needs only the Bitcoin address of the receiving party and the sender's own private key. This information on its own rarely reflects any identifying information about either the sender or the recipient. As a result, little-to-no personally identifiable information about the sender or recipient is transmitted in a Bitcoin transaction itself. Once the sender's transaction announcement is verified by the network, the transaction is added to the blockchain, a decentralized public ledger that records every Bitcoin transaction. The blockchain logs every Bitcoin address that has ever received bitcoin and maintains records of every transaction for each Bitcoin address.

17. While a Bitcoin address owner's identity is generally anonymous within the blockchain (unless the owner chooses to make information about the owner's Bitcoin address publicly available), investigators can often use the blockchain to identify the owner of a particular Bitcoin address. Because the blockchain serves as a searchable public ledger of every Bitcoin transaction, investigators can trace transactions to, among other recipients, virtual currency exchanges.

REVIEWING THE BITCOIN PUBLIC LEDGER

18. The Bitcoin public ledger can be accessed from any computer connected to the internet simply by searching for it in a search program like Google. As noted above, the entire Bitcoin public ledger is stored on most of the computers that make up the peer-to-peer network.

19. Importantly, once a Bitcoin address is used, it becomes traceable by the history of all transactions that the address is involved with. Anyone can see the balance and all transactions of any

address. This information is part of the public ledger.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief. Executed this 28th day of July, 2021 in East Lansing, Michigan.

_____/s/_____
JEREMIAH HAYNIE
Special Agent
Internal Revenue Service – Criminal Investigation